Docket No. 0918.0011C

EDELL, SHAPIRO & FINNAN, LLC
1901 Research Boulevard
Suite 400
Rockville, Maryland 20850-3164
(301) 424-3640

In re the PATENT application of

Edwin H. Wrench, Jr.

Serial No.: 09/731,836

Filed: December 8, 2000

Technology Center: 2100

Group Art Unit: 2137

Examiner: Pyzocha, Michael J.

Confirmation No.: 1865

For: Method and Apparatus to Facilitate Secure Network Communications with a Voice Responsive Network Interface Device

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Sir:

Transmitted herewith for filing in the subject application is Appellant's Brief (40 pages);

Check #9854 in the amount of $500.00 in payment of the Brief filing fee.

The Commissioner is hereby authorized to charge payment of any additional fees required

for the above-identified application or Assignment or credit any overpayment to Deposit Account

No. 05-0460.

Respectfully submitted,

Stuart B. Shapiro
Registration No. 40,169

Hand-delivered: ___August 2, 2006___

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the PATENT application of

Edwin H. Wrench, Jr.

Serial No.: 09/731,836	Group Art Unit: 2137
Filed: December 8, 2000	Examiner: Pyzocha, Michael J.
Technology Center: 2100	Confirmation No.: 1865

For: Method and Apparatus to Facilitate Secure Network Communications with a Voice Responsive Network Interface Device

APPEAL BRIEF

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is presented pursuant to the Notice of Appeal filed on April 3, 2006 and the Extensions of Time filed on June 2, 2006 and July 5, 2006 extending the deadline for filing the Appeal Brief to August 3, 2006. The brief is filed pursuant to the requirements of 37 C.F.R. §41.37.

(1)   <u>Real Party in Interest</u>

The current patent owner or real party in interest is ITT Manufacturing Enterprises, Inc., the assignee of record, which is a corporation duly organized and existing under the laws of the state of Delaware and having a place of business at 1105 North Market Street, Suite 1217, Wilmington, Delaware, 19801.

(2)   Related Appeals and Interferences

Appellant is currently unaware of any prior and pending appeals, judicial proceedings or interferences which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3)   Status of Claims

Claims 31 - 36 have been canceled.

Claims 1 - 30 are currently rejected under 35 U.S.C. §103(a).

(4)   Status of Amendments

An after-final amendment was filed May 24, 2006 which included proposed modifications to the claims in response to claim objections in the Office Action of January 6, 2006. The Examiner responded with an Advisory Action dated June 12, 2006 denying entry of the claim amendments. A second after-final amendment was filed June 14, 2006 which included proposed modifications to the claims in response to claim objections in the Office Action of January 6, 2006. The Examiner responded with an Advisory Action dated July 31, 2006 indicting entry of the amendment, withdrawal of the claim objections and rejection of claims 1 - 30 under 35 U.S.C. §103(a).

(5)   Summary of Claimed Subject Matter

The present invention and claimed subject matter are directed toward a system for facilitating secure encrypted communications over a network with a network interface providing unencrypted sessions with web sites (e.g., See Specification Page 8, Lines 22 - 25). The system includes a

security system 4 utilized in conjunction with a voice browser system 2 (e.g., See Fig. 1; Specification Page 5, Lines 20 - 23; and Page 7, Lines 8 - 11) and a security module 6 for voice browser system 2 that creates a secure connection to security system 4 (e.g., See Figs. 1 and 4; Specification Page 5, Lines 23 - 25; Page 8, Lines 25 - 28; Page 9, Lines 16 - 22; and Page 12, Lines 21 - 25).

In order to enable retrieval of user security related information stored in a database 8 remote from voice browser system 2, the user provides an identification to voice browser system 2 that is transferred to and verified by security system 4 (e.g., See Figs. 1 - 4; Specification Page 5, Lines 25 - 27; Page 10, Lines 9 - 26; Page 11, Lines 14 - 23; and Page 12, Lines 25 - 28). Once the identification is verified, the user is prompted by voice browser system 2 to speak a phrase for voice verification. The verification speech signals are transferred from voice browser system 2 to security system 4 to verify those speech signals against speech signals of a particular authorized user associated with the identification and stored in remote database 8 (e.g., See Figs. 1 - 4; Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 11, Lines 24 - 26; Page 12, Lines 8 - 17; and Page 12, Line 28 to Page 13, Line 3).

When the user is verified, security system 4 retrieves a user private key and certificate from database 8 remote from voice browser system 2 (e.g., See Figs. 3 - 4; Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 13).

In response to the user subsequently accessing a web site residing on a secure server 12, the

3

secure server and voice browser system 2 initiate a secure key exchange. Data packets from secure server 12 containing security information are identified by security module 6 of voice browser system 2 and transferred to security system 4 for processing, while security information from security system 4 is transferred to secure server 12 via voice browser system 2. The resulting session key is securely transferred to voice browser system 2 to facilitate secure communications between voice browser system 2 and secure server 12 (e.g., See Figs. 1, 5 - 7; Specification Page 6, Lines 2 - 10; Page 14, Line 30 to Page 16, Line 14).

In other words, security module 6 intercepts security information received by voice browser system 2 from secure server 12 in response to the voice browser system accessing a secure web site, and transmits the security information to security system 4 to handle processing of the security information for voice browser system 2. This enables voice browser system 2 to conduct a secure session or provide secure communications with a secure web site of secure web server 12. The present invention embodiments further include a method, a program product apparatus and a carrier signal (with embedded computer program logic) (e.g., See Specification Page 18, Line 29 to Page 19, Line 3) for facilitating secure encrypted communications over a network as described above.

(6)   Grounds of Rejection to be Reviewed on Appeal

(A) Whether claims 1 - 9, 11 - 28 and 30 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent No. 6,484,263 (Liu), further in view of U.S. Patent No. 5,953,700 (Kanevsky et al.), further in view of U.S. Patent No. 6,266,418 (Carter et al.) and further in view of U.S. Patent No. 6,560,576 (Cohen et al.).

(B)   Whether claims 10 and 29 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent

No. 6,484,263 (Liu), further in view of U.S. Patent No. 5,953,700 (Kanevsky et al.), further in view

of U.S. Patent No. 6,266,418 (Carter et al.), further in view of U.S. Patent No. 6,560,576 (Cohen et

al.) and further in view of U.S. Patent No. 5,341,426 (Barney et al.).

(7)   <u>Argument</u>

(A) <u>Rejection of Claims 1 - 9, 11 - 28 and 30 under 35 U.S.C. §103(a)</u>

In the Office Action of January 6, 2006, the Examiner rejected claims 1 - 9, 11 - 28 and 30

under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,484,263 (Liu), further in view

of U.S. Patent No. 5,953,700 (Kanevsky et al.), further in view of U.S. Patent No. 6,266,418 (Carter

et al.) and further in view of U.S. Patent No. 6,560,576 (Cohen et al.). These rejections were

maintained in the Advisory Actions of June 12, 2006 and July 31, 2006.

(A.1) <u>Legal Analysis for Obviousness</u>

35 U.S.C. §103(a) states (in pertinent part):

"(a)   A patent may not be obtained though the invention is not identically disclosed or
        described as set forth in section 102 of this title, if the differences between the subject
        matter sought to be patented and the prior art are such that the subject matter as a
        whole would have been obvious at the time the invention was made to a person
        having ordinary skill in the art to which said subject matter pertains..."

The Supreme Court in <u>Graham v. John Deere</u>, 148 U.S.P.Q. 459 (1966), stated that the

obviousness or non-obviousness of subject matter is determined in view of the scope and content of

the prior art, the differences between the prior art and the claims at issue and the level of ordinary

skill in the pertinent art. Secondary considerations, such as commercial success, long felt but

unsolved needs, failure of others, etc., might be utilized to give light to the circumstances

surrounding the origin of the subject matter sought to be patented. See M.P.E.P. §2141.

The following tenets of patent law must be adhered to when applying 35 U.S.C. §103:

(i) The claimed invention must be considered as a whole;

(ii) The references must be considered as a whole and must suggest the desirability and thus

the obviousness of making the combination;

(iii) The references must be viewed without the benefit of impermissible hindsight vision

afforded by the claimed invention; and

(iv) Reasonable expectation of success is the standard with which obviousness is determined.

Hodosh v. Block Drug Co., Inc., 229 U.S.P.Q. 182, 187 n.5 (Fed. Cir. 1986); See M.P.E.P. §2141.

The basic criteria to establish a prima facie case of obviousness, include: some suggestion or

motivation, either in the references themselves or in the knowledge generally available to one of

ordinary skill in the art, to modify the reference or to combine reference teachings; a reasonable

expectation of success; and the prior art reference (or references when combined) must teach or

suggest all the claim limitations. The teaching or suggestion to make the claimed combination and

the reasonable expectation of success must both be found in the prior art, not in applicant's

disclosure. In re Vaeck, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); See M.P.E.P. §2142. Three possible

sources for a motivation to combine references include the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. In re Rouffet, 47 U.S.P.Q.2d 1453, 1457-58 (Fed. Cir. 1998); See M.P.E.P. §2143.01.

(A.2) Claims 1 - 6, 9, 11 - 12, 15 - 16, 19 - 25, 28 and 30 are Patentable Over the Combination of the Liu et al., Kanevsky et al., Carter et al. and Cohen et al. Patents

Initially, independent claims 1, 12, 16 and 20 each recite the features of:

(i)   facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites and including a voice browser;

(ii)   a security module to detect a secure web server providing encrypted sessions and identify security related information received by the network interface from the secure web server in response to the voice browser accessing a secure web site of the secure web server based on voice commands from a user, wherein the security related information includes information enabling a secure encrypted session with the secure web server;

(iii)   voice and security information associated with authorized users and stored remotely from the network interface, wherein the security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers; and

(iv)   a security system (or secure communications module) processing for the network interface the identified security related information to enable the secure encrypted session, wherein a user is verified based on a comparison of user voice signals with the remotely stored voice

information, the security information of a verified user is retrieved from the remote location, and communication parameters are negotiated with the secure web server utilizing the retrieved security information to facilitate the secure encrypted session between the secure web server and the voice browser.

The Examiner takes the position that the Liu et al. patent discloses the claimed subject matter, except for the authorization being a comparison of the user voice signals with stored voice information being stored remotely, negotiating encryption parameters for a secure session, and detecting a secure web connection and providing the encrypted sessions. The Examiner further alleges that these features are disclosed by the Kanevsky et al., Carter et al. and Cohen et al. patents, respectively, and that it would have been obvious to combine the patents to attain the claimed invention.

Specifically, the Examiner concedes at Page 4 of the Office Action of January 6, 2006 that the modified Liu, Kanevsky et al. and Carter et al. system fails to disclose "detecting a secure web connection and providing the encrypted session". The Examiner takes the further position that the Cohen et al. patent teaches detecting an event in a voice browser.

However, the broad assertion of detecting an event is not a disclosure of the claimed feature of detecting a secure web connection or, more precisely, the security module detecting a secure web server providing encrypted sessions and identifying security related information received by the network interface from the secure web server in response to the voice browser accessing a secure web site of the secure web server based on voice commands from a user as recited in the independent claims. The Cohen et al. patent does not disclose, teach or suggest this claimed feature, but rather, is

8

directed toward a voice enabled application, which may be a voice browser, that is configured to provide active help to a user. The application maintains a number of active help prompts capable of being played to a user as speech, and a number of sets of conditions, each set corresponding to a different active help prompt relating to use of the voice browser (e.g., See Abstract; Column 3, line 62 to Column 4, line 7; and Tables from Columns 9 to 14). Dialog states are monitored by event listeners configured to detect an event "thrown" (i.e., signaled or generated) in response to a specified transition between dialog states. A dialog state is expressly defined as a single interchange, starting with a prompt and ending with the caller's response or an action that does not require a response (e.g., See Column 6, lines 42 - 45 and lines 48 - 53). In response to a thrown event, certain conditions related to an active help prompt are applied (e.g., See Abstract; Column 4, Lines 1 - 5; and Column 6, lines 53 - 55). A prompt is played to the user if the applied conditions are satisfied (e.g., See Abstract; Column 4, lines 3 - 7; and Column 6, lines 56 - 58).

Thus, the Cohen et al. patent discloses monitoring an exchange between a user and a voice browser and playing a help prompt to the user assisting with use of voice browser functions based on the particular user exchange and in response to certain conditions being satisfied. There is no disclosure, teaching or suggestion of detecting a secure web connection and providing encrypted sessions for a voice browser as recited in the independent claims. Accordingly, the proposed combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents does not disclose, teach or suggest each and every feature recited in independent claims 1, 12, 16 and 20.

In addition to the foregoing, the Liu, Kanevsky et al. and Carter et al. patents do not disclose features within the claims (and fail to compensate for the deficiencies of the Cohen et al. patent).

9

Initially, the present invention (and claims) are directed toward a security system to serve as a proxy in order to handle processing of secure encrypted sessions for a network interface including a voice browser that is otherwise incapable of accommodating such sessions. This is accomplished by a security module for the network interface to identify security information pertaining to secure encrypted sessions received from secure web servers, and a security system to process the identified security information to establish the encrypted session for the network interface as described above.

The Examiner has utilized various documents in this rejection as alleged teachings of various individual claimed features, such as encrypted sessions and detection thereof, remote storage and voice authentication. However, none of the cited documents disclose the claimed feature of a proxy to handle processing to establish a secure encrypted session for a voice browser (otherwise incapable of accommodating the secure session).

In particular, the Liu patent discloses a system and method for accessing password protected web sites through web browsers without manually supplying a username and password by users. A system arrangement is disclosed allowing a telephone user to access Web pages residing on Internet Web servers. The system includes a telephone coupled to an IVR platform via a PSTN. The IVR interfaces with the Internet to which a phone browser and Web browser are connected. A telephone call is picked up at the IVR which determines a URL based on the telephone number dialed. A session is established with the phone browser which is initialized with the URL. The phone browser interacts with the Web server hosting the destined URL. The information obtained from the Web server is sent to the IVR for conversion and audible presentation to the caller (e.g., See Figs. 1 - 2; and Column 1, line 44 to Column 2, line 21). The browser maintains, for each user, one user

10

security profile which stores the URLs and the corresponding log-in username and password. When the browser receives a username-password challenge from the Web server, the browser first searches the user security profile for the URL the challenge is received from. If a match is found, the browser sends the challenging Web server the user name and password that is associated with the matched URL (e.g., See Abstract; and Column 3, Lines 36 - 64). The browser may alternatively be implemented by voice type browsers (e.g., See Column 3, Lines 36 - 43).

Thus, the Liu patent discloses a browser providing a locally stored username and password to access a password protected web site in response to a challenge from that web site (e.g., See Fig. 2 and Column 3, lines 48 - 52). In other words, the Liu patent is directed toward access of password protected sites and provides no disclosure whatsoever for secure encrypted sessions. Accordingly, there is no disclosure, teaching, or suggestion of the browser identifying security related information that enables a secure encrypted session and is received by a network interface from a secure web server in response to accessing a secure web site of the secure web server, or a security system to receive and process the identified security information for the browser to enable the secure encrypted session for the browser as recited in the independent claims.

The Kanevsky et al. patent discloses a portable acoustic signal preprocessing device for accessing an automatic speech/speaker recognition server to perform speech and speaker recognition at a remote location (e.g., See Abstract). The device includes a microphone to receive sound including speech spoken by the user, an analog to digital converter which converts the analog electrical signal from the microphone to digitized signals, and a digital signal processor (DSP) to process data and control data flow in the portable device. The functions of the DSP include:

preprocessing the speech data spoken into the microphone into feature vectors (or "feature data"); processing silence and background noise data to assist in establishing or estimating the transfer function of the communication channel; and performing other functions including coordination of transmission and reception of data to and from the portable device, encrypt/decrypt, and compress/decompress data if necessary (e.g., See Column 3, lines 45 - 66). Data processed by the DSP is output to an acoustic coupler, wherein the digital data are converted to audio signals. As such, the audio signals from the acoustic coupler could be played or spoken into an audio communication device, such as a standard telephone handset, for transmission over an audio communication channel, such as a telephone line (e.g., See Column 4, Lines 8 - 13).

Encryption/decryption and compression/decompression devices are optional components of the portable device. The encryption/decryption device encrypts the data preprocessed by the DSP with a preestablished encryption key to provide secure transaction of the signals over the telephone line (e.g., See Column 4, Lines 33 - 41). The speech/speaker recognition server is located remotely from the portable device. The server performs speech/speaker recognition on the preprocessed signals received from the portable device (e.g., See Column 5, Lines 34 - 67).

Thus, the Kanevsky et al. patent discloses a device that preprocesses speech signals from a user for remote speech/speaker recognition. Although the speech information may be encrypted, the communication is between the portable device and speech/speaker recognition server and there is no disclosure, teaching or suggestion of secure encrypted sessions between voice browsers and web sites of secure servers, or identifying security related information for transfer to a proxy system to establish the secure encrypted sessions for a voice browser as recited in the independent claims.

The Carter et al. patent is directed toward an encryption device for a telephone having a handset and a base unit. The device includes a handset interface, a first converter, an encryption processor, a second converter, and a host interface. The handset interface receives analog output signals from the handset. The first converter converts the analog output signals into digital output signals. The encryption processor includes a compressor, a key manager, an encryptor, and a modulator. The key manager generates key material for encrypting the digital output signals. The compressor compresses the digital output signals, the encryptor encrypts the digital output signals based on the key material, and the modulator modulates the encrypted digital output signals. The second converter converts the encrypted digital output signals into encrypted analog output signals. The host interface receives encrypted analog output signals from the encryption processor and forwards the encrypted analog output signals to the base unit (e.g., See Abstract).

Regardless of the type of host telephone or network, the device receives analog output signals (i.e., audio, such as voice) from a microphone in the handset, and then digitizes, compresses, and encrypts the output signals. The output signals are then converted back to analog tones. The analog tones are forwarded over the telephone network to which the host telephone is connected to a second host telephone comprising a second device. When received at the second device, the analog tones are demodulated and decrypted into compressed audio. The compressed audio is then expanded and converted back to an analog signal, which is driven out to the handset's earpiece. The identical process is also performed in the reverse direction within each device. The result is a full-duplex telephone conversation that is immune from eavesdropping with no degradation in speech quality (e.g., See Column 3, Lines 40 - 55).

Thus, the Carter et al. patent is directed toward a device that can be connected between the handset and base unit of any of a variety of ordinary telephones to provide secure, full-duplex telephone conversations that are immune from eavesdropping with no degradation in speech quality (e.g., See Column 1, lines 51 – 55). Although the audio information may be encrypted and a secure session established, the communication and session is established between telephones. There is no disclosure, teaching or suggestion of secure encrypted sessions between voice browsers and web sites of secure servers, or identifying security related information for transfer to a proxy system to establish the secure encrypted sessions for a voice browser as recited in the independent claims. In fact, the secure communications within the Carter et al. patent is handled directly by the communicating devices.

Since the proposed combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents does not disclose, teach or suggest each and every feature recited in independent claims 1, 12, 16 and 20 as discussed above, the rejection is considered improper.

Claims 2 - 6, 9, 11, 15, 19, 21 - 25, 28 and 30 depend, either directly or indirectly, from independent claims 1, 12, 16 or 20 and, therefore, include all the limitations of their parent claims. These claims are considered to overcome the combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents for substantially the same reasons discussed above in relation to their parent claims and for further limitations recited in these claims.

In addition to the foregoing, there is no apparent reason or motivation to combine the teachings of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents. In particular, the Liu patent is directed toward entering information (i.e., username and password) from a non-GUI

interface when accessing a password protected Web site (e.g., See Column 2, Lines 39 - 41 and Lines 48 - 50) as described above. The Kanevsky et al. patent is directed toward preprocessing of speech information at a client's end to enhance speech recognition accuracy (e.g., See Column 1, Lines 56 - 59; and Column 2, Lines 5 - 13) as described above. The Carter et al. patent is directed toward providing secure telephone communications on public or private networks without interfering with proprietary services (e.g., See Column 1, Lines 40 - 55) as described above. The Cohen et al. patent is directed toward a voice enabled application, which may be a voice browser, that is configured to provide active help to a user as described above. Since the patents are directed toward diverging applications as discussed above, there is no apparent reason, motivation or suggestion to combine their teachings absent prohibited hindsight derived from Applicant's own disclosure. In addition, none of the patents recognize or address the problem solved by the present invention of enabling voice browsers to conduct secure encrypted sessions with web sites. Accordingly, the proposed combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents does not render the claimed invention obvious.

(A.3)   Claims 7 - 8, 13 - 14, 17 - 18 and 26 - 27 are Patentable Over the Combination of

the Liu et al., Kanevsky et al., Carter et al. and Cohen et al. Patents

Initially, claims 7 - 8, 13 - 14, 17 - 18 and 26 - 27 depend, either directly or indirectly, from independent claims 1, 12, 16 or 20 and, therefore, include all the limitations of their parent claims. These claims are considered to overcome the combination of the Liu, Kanevsky et al., Carter et al.

and Cohen et al. patents for substantially the same reasons discussed above in relation to their parent claims and for further limitations recited in the dependent claims.

In particular, dependent claims 7, 13 and 17 further recite the features of the security module: identifying security related information received by the network interface from the secure web server; facilitating communications with the security system (or secure communications module) and the network interface; providing the user information and the identified security information to the security system (or secure communications module) to facilitate verification of the user and negotiation of the communication parameters; receiving a request for the user information, verification results, responses to the identified security information and the negotiated communication parameters from the security system (or secure communications module); and providing the responses and the negotiated parameters to the network interface to facilitate secure communications over the network between the secure web server and the voice browser.

Dependent claim 26 further recites the features of the security module: providing user information to the security system to facilitate verification of the user in response to a request from the security system for user information; receiving verification results from the security system and providing the verification results to the user; providing identified security information to the security system to facilitate negotiation of communication parameters; receiving responses to the identified security information and the negotiated communication parameters from the security system; and providing the responses and the negotiated parameters to the network interface to facilitate secure communications over the network between the secure web server and the voice browser.

Dependent claims 8, 14 and 18 depend from claims 7, 13 and 17, respectively, and further

recite the features of the security system (or secure communications module): generating a user information request including a request for user information corresponding to selected portions of retrieved voice information; comparing user voice signals received from the security module in response to the user information request with stored voice information; processing identified security information received from the security module and generating responses thereto with retrieved security information to negotiate communication parameters; providing the user information request, verification results, generated responses and negotiated parameters to the security module; and receiving user voice signals and the identified security information from the security module.

Dependent claim 27 depends from claim 26 and further recites the features of the security system: generating a user information request including a request for user information corresponding to selected portions of retrieved voice information; comparing user voice signals received from the security module in response to the user information request with stored voice information; processing identified security information received from the security module and generating responses thereto with retrieved security information to negotiate communication parameters; and providing verification results, responses and negotiated parameters to the security module to facilitate secure communications over the network between the secure web server and the voice browser.

The Examiner takes the position that the combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents discloses the features of independent claims 1, 12, 16 and 20, and that the further features of dependent claims 7 - 8, 13 - 14, 17 - 18 and 26 - 27 are disclosed by the Liu patent

as modified by the Kanevsky et al. and Carter et al. patents with respect to the independent claims.

However, the above features within the dependent claims are directed toward the communications, exchanges and/or interactions between the security module and security system (or secure communications module) (e.g., containing information relating to the identified security information, user voice signals, user information request, verification results, responses to the identified security information, negotiated communication parameters, etc.) to enable establishment of the secure session between the voice browser and secure web server. Since the combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents does not disclose the claimed feature of a proxy to handle processing to establish a secure encrypted session between a voice browser and web site of a secure web server as discussed above, the further features recited in the dependent claims directed toward the specified communications, exchanges and/or interactions between the security module and security system (or secure communications module) are similarly not disclosed, taught or suggested by that combination. Accordingly, dependent claims 7 - 8, 13 - 14, 17 - 18 and 26 - 27 are considered to overcome the rejection.

(B) Rejection of Claims 10 and 29 under 35 U.S.C. §103(a)

In the Office Action of January 6, 2006, the Examiner rejected claims 10 and 29 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,484,263 (Liu), further in view of U.S. Patent No. 5,953,700 (Kanevsky et al.), further in view of U.S. Patent No. 6,266,418 (Carter et al.), further in view of U.S. Patent No. 6,560,576 (Cohen et al.) and further in view of U.S. Patent No. 5,341,426 (Barney et al.). These rejections were maintained in the Advisory Actions of June 12,

2006 and July 31, 2006.

(B.1) Claims 10 and 29 are Patentable Over the Combination of the Liu et al., Kanevsky et al., Carter et al., Cohen et al. and Barney et al. Patents

As discussed above, the obviousness or non-obviousness of subject matter is determined in view of the scope and content of the prior art, the differences between the prior art and the claims at issue and the level of ordinary skill in the pertinent art. Secondary considerations, such as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. Further, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure.

Initially, claims 10 and 29 depend, either directly or indirectly, from independent claims 1 and 20, respectively, and therefore include all the limitations of their parent claims. These claims are considered to overcome the combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents for substantially the same reasons discussed above in relation to their parent claims.

Claims 10 and 29 further recite the feature of the stored security information including private keys and certificates of authorized users.

The Examiner takes the position that the combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents discloses the claimed subject matter, except for stored security information including private keys and certificates of authorized system users. The Examiner further alleges that

the Barney et al. patent discloses this feature and that it would have been obvious to combine the Liu, Kanevsky et al., Carter et al., Cohen et al. and Barney et al. patents to attain the claimed invention.

However, the combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents does not disclose the claimed feature of a proxy to handle processing to establish a secure encrypted session between a voice browser and web site of a secure web server as discussed above.

Further, the Barney et al. patent does not compensate for the deficiencies of the combination of the Liu, Kanevsky et al., Carter et al. and Cohen et al. patents, but rather, is directed toward a secure communication system comprising a data communications network, data links, and first and second communications terminals, as for example, secure telephones. Input data are encrypted in the terminals and subsequently transmitted via the data links and data communications network to, for example, another one of a secure communications terminal, wherein the encryption and digitizing processes are reversed, providing plain-text data equivalent to the original input data. The system provides within one or both of the terminals an apparatus and method for rapidly initiating the encrypting and decrypting of messages according to one of several possible protocols that both terminals can understand (e.g., See Fig. 1; and Column 3, Line 51 to Column 4, line 26).

A method for establishing a secure communications link between the first and second terminals includes exchanging a first message containing information describing encryption devices and communications modes available within the terminals and user authentication information, selecting, in at least one terminal, a common key generation and ciphering algorithm, exchanging a second message for providing data to form traffic keys, exchanging a third message for synchronizing secure communications, and initiating secure communication (e.g., See Figs. 2, 4 and

5; Abstract; Column 4, Lines 27 - 52; and Column 6, Lines 43 - 60). A key certification authority provides keys to the secure terminals during an initial key certification phase. The secure terminals utilize the keys to exchange the messages for establishing secure communications. This provides an authenticated authorization for the terminals to engage in the secure communications (e.g., See Fig. 3; Column 4, Line 65 to Column 5, Line 5; and Column 5, Lines 33 - 35 and 57 - 65).

Although the Barney et al. patent discloses exchanging messages to establish a secure session between terminals, there is no disclosure, teaching or suggestion of identifying security related information for transfer to a proxy system to establish a secure encrypted session between a voice browser and a web site of a secure server as recited in the claims. In fact, the secure communications and exchange of messages within the Barney et al. patent is handled directly by the communicating terminals. The Barney et al. patent is merely utilized by the Examiner for an alleged teaching of private keys and certificates.

Since the proposed combination of the Liu, Kanevsky et al., Carter et al., Cohen et al. and Barney et al. patents does not disclose, teach or suggest each and every feature recited in claims 10 and 29 as discussed above, this rejection is considered improper.

In addition to the foregoing, there is no apparent reason or motivation to combine the Barney et al. patent with the teachings of the Liu, Kanevsky et al., Carter et al., and Cohen et al. patents. In particular, the Liu patent is directed toward entering information (i.e., username and password) from a non-GUI interface when accessing a password protected Web site as described above. The Kanevsky et al. patent is directed toward preprocessing of speech information at a client's end to

21

enhance speech recognition accuracy as described above. The Carter et al. patent is directed toward providing secure telephone communications on public or private networks without interfering with proprietary services as described above. The Cohen et al. patent is directed toward a voice enabled application, which may be a voice browser, that is configured to provide active help to a user as described above. The Barney et al. patent is directed toward providing a manner to rapidly establish authenticated traffic keys for use in low bit rate secure communications systems (e.g., See Column 1, Lines 35 - 38 and 51 - 53). Thus, the patents are directed toward diverging applications and there is no apparent reason, motivation or suggestion to combine their teachings absent prohibited hindsight derived from Applicant's own disclosure. In addition, none of the patents recognize or address the problem solved by the present invention of enabling voice browsers to conduct secure encrypted sessions with web sites of secure servers. Accordingly, the proposed combination of the Liu, Kanevsky et al., Carter et al., Cohen et al. and Barney et al. patents does not render the claimed invention obvious.

(8) <u>Claims Appendix</u>

1.   A system for facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites, wherein said network interface includes a voice browser for receiving voice signals from a user and accessing and navigating web sites in accordance with said received voice signals, said system comprising:

a security module for said network interface to facilitate retrieval of information from said user in the form of voice signals and to detect a secure web server providing encrypted sessions and identify security related information received by said network interface from said secure web server in response to said voice browser accessing a secure web site of said secure web server based on voice commands from said user, wherein said security related information includes information enabling a secure encrypted session with said secure web server;

a storage unit to store remote from said network interface voice and security information associated with authorized users of said system, wherein said security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers; and

a security system to communicate with said security module and said storage unit and to process for said network interface said identified security information to enable said secure encrypted session, wherein said security system includes:

a verification module to verify said user as an authorized system user based on a comparison of said user voice signals with said stored voice information;

a retrieval module to retrieve said security information of said verified user from said storage unit; and

a negotiation module to receive said identified security information from said security module and negotiate communication parameters with said secure web server utilizing said retrieved security information to facilitate said secure encrypted session between said secure web server and said voice browser.

2. The system of claim 1 wherein said network includes the Internet.

3. The system of claim 1 wherein said network interface is in communication with a communications device located remotely of said network interface, and said security module facilitates retrieval of said user voice signals from said communications device.

4. The system of claim 3 wherein said communications device includes a telephone.

5. The system of claim 3 wherein said communications device includes a computer system having an audio input device.

6. The system of claim 5 wherein said audio input device includes a microphone.

7. The system of claim 1 wherein said security module includes:

an identification module to identify said security related information received by said network interface from said secure web server;

a communications module to facilitate communications with said security system and said network interface, wherein said communications module includes:

a send module to provide said user information and said identified security information to said security system to facilitate verification of said user and negotiation of said communication parameters;

a receive module to receive a request for said user information, verification results, responses to said identified security information and said negotiated communication parameters from said security system; and

an interface module for providing said responses and said negotiated parameters to said network interface to facilitate secure communications over said network between said secure web server and said voice browser; and

a user interface module to facilitate said user information request for retrieval of said user information and to provide said verification results to said user.

8.   The system of claim 7 wherein said security system further includes:

an identification verification module to validate an identification within said user information associated with an authorized system user;

an access module to retrieve said voice information from said storage unit associated with said identification;

a selection module to select portions of said retrieved voice information and generate said user information request, wherein said generated request includes a request for user information corresponding to said selected portions of said retrieved voice information, and wherein said verification module verifies said user by comparing said user voice signals received from said security module in response to said user information request with said stored voice information associated with an authorized user identified by said identification and said negotiation module processes said identified security information received from said security module and generates said responses thereto with said retrieved security information to negotiate said communication parameters; and

a security communications module to facilitate communications with said security module, wherein said security communications module includes:

a security send module to provide said user information request, said verification results, said generated responses and said negotiated parameters to said security module; and

a security receive module to receive said user voice signals and said identified security information from said security module.

9. The system of claim 1 wherein said storage unit includes a database.

10.   The system of claim 2 wherein said stored security information includes private keys and certificates of said authorized system users.

11.   The system of claim 1 further including:

an enrollment module to retrieve voice signals from said authorized system users and process said authorized system user voice signals to produce said voice information for storage in said storage unit.

12.   A program product apparatus having a computer readable medium with computer program logic recorded thereon for facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites, wherein said network interface includes a voice browser for receiving voice signals from a user and accessing and navigating web sites in accordance with said received voice signals, said program product apparatus comprising:

a security module for said network interface to facilitate retrieval of information from said user in the form of voice signals and to detect a secure web server providing encrypted sessions and identify security related information received by said network interface from said secure web server in response to said voice browser accessing a secure web site of said secure web server based on voice commands from said user, wherein said security related information includes information enabling a secure encrypted session with said secure web server;

a storage module to store remote from said network interface voice and security information associated with authorized users, wherein said security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers; and

a secure communications module for a security system to communicate with said security module and said storage module and to process for said network interface said identified security information to enable said secure encrypted session, wherein said secure communications module includes:

a verification module to verify said user as an authorized user based on a comparison of said user voice signals with said stored voice information;

a retrieval module to retrieve said security information of said verified user from said storage module; and

a negotiation module to receive said identified security information from said security module and negotiate communication parameters with said secure web server utilizing said retrieved security information to facilitate said secure encrypted session between said secure web server and said voice browser.

13. The program product apparatus of claim 12 wherein said security module includes:

an identification module to identify said security related information received by said network interface from said secure web server;

a communications module to facilitate communications with said secure communications module and said network interface, wherein said communications module includes:

a send module to provide said user information and said identified security information to said secure communications module to facilitate verification of said user and negotiation of said communication parameters;

a receive module to receive a request for said user information, verification results, responses to said identified security information and said negotiated communication parameters from said secure communications module; and

an interface module for providing said responses and said negotiated parameters to said network interface to facilitate secure communications over said network between said secure web server and said voice browser; and

a user interface module to facilitate said user information request for retrieval of said user information and to provide said verification results to said user.

14. The program product apparatus of claim 13 wherein said secure communications module further includes:

an identification verification module to validate an identification within said user information associated with an authorized user;

an access module to retrieve said voice information from said storage module associated with said identification;

a selection module to select portions of said retrieved voice information and generate said user information request, wherein said generated request includes a request for user information

corresponding to said selected portions of said retrieved voice information, and wherein said verification module verifies said user by comparing said user voice signals received from said security module in response to said user information request with said stored voice information associated with an authorized user identified by said identification and said negotiation module processes said identified security information received from said security module and generates said responses thereto with said retrieved security information to negotiate said communication parameters; and

a security communications module to facilitate communications with said security module, wherein said security communications module includes:

a security send module to provide said user information request, said verification results, said generated responses and said negotiated parameters to said security module; and

a security receive module to receive said user voice signals and said identified security information from said security module.

15.   The program product apparatus of claim 12 further including:

an enrollment module to retrieve voice signals from said authorized users and process said authorized user voice signals to produce said voice information for storage in said storage module.

16.   A carrier signal having computer program logic embedded therein causing an apparatus to facilitate secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites, wherein said network interface includes

a voice browser for receiving voice signals from a user and accessing and navigating web sites in accordance with said received voice signals, said carrier signal comprising:

a security module for said network interface to facilitate retrieval of information from said user in the form of voice signals and to detect a secure web server providing encrypted sessions and identify security related information received by said network interface from said secure web server in response to said voice browser accessing a secure web site of said secure web server based on voice commands from said user, wherein said security related information includes information enabling a secure encrypted session with said secure web server;

a storage module to store remote from said network interface voice and security information associated with authorized users, wherein said security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers; and

a secure communications module for a security system to communicate with said security module and said storage module and to process for said network interface said identified security information to enable said secure encrypted session, wherein said secure communications module includes:

a verification module to verify said user as an authorized system user based on a comparison of said user voice signals with said stored voice information;

a retrieval module to retrieve said security information of said verified user from said storage module; and

a negotiation module to receive said identified security information from said security module and negotiate communication parameters with said secure web server utilizing said retrieved security information to facilitate said secure encrypted session between said secure web server and said voice browser.

17.   The carrier signal of claim 16 wherein said security module includes:

an identification module to identify said security related information received by said network interface from said secure web server;

a communications module to facilitate communications with said secure communications module and said network interface, wherein said communications module includes:

a send module to provide said user information and said identified security information to said secure communications module to facilitate verification of said user and negotiation of said communication parameters;

a receive module to receive a request for said user information, verification results, responses to said identified security information and said negotiated communication parameters from said secure communications module; and

an interface module for providing said responses and said negotiated parameters to said network interface to facilitate secure communications over said network between said secure web server and said voice browser; and

a user interface module to facilitate said user information request for retrieval of said user information and to provide said verification results to said user.

18.   The carrier signal of claim 17 wherein said secure communications module includes:

an identification verification module to validate an identification within said user information associated with an authorized user;

an access module to retrieve said voice information from said storage module associated with said identification;

a selection module to select portions of said retrieved voice information and generate said user information request, wherein said generated request includes a request for user information corresponding to said selected portions of said retrieved voice information, and wherein said verification module verifies said user by comparing said user voice signals received from said security module in response to said user information request with said stored voice information associated with an authorized user identified by said identification and said negotiation module processes said identified security information received from said security module and generates said responses thereto with said retrieved security information to negotiate said communication parameters; and

a security communications module to facilitate communications with said security module, wherein said security communications module includes:

a security send module to provide said user information request, said verification results, said generated responses and said negotiated parameters to said security module; and

a security receive module to receive said user voice signals and said identified security information from said security module.

19.   The carrier signal of claim 16 further including:

an enrollment module to retrieve voice signals from said authorized users and process said authorized user voice signals to produce said voice information for storage in said storage module.

20.   A method of facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites, wherein said network interface includes a voice browser for receiving voice signals from a user and accessing and navigating web sites in accordance with said received voice signals, said method comprising:

(a)   retrieving, via a security module, information from said user in the form of voice signals and detecting a secure web server providing encrypted sessions and identifying security related information received by said network interface from said secure web server in response to said voice browser accessing a secure web site of said secure web server based on voice commands from said user, wherein said security related information includes information enabling a secure encrypted session with said secure web server;

(b)   storing remote from said network interface voice and security information associated with authorized users in a storage unit, wherein said security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers;

(c)   verifying said user as an authorized user based on a comparison of said user voice signals with said stored voice information via a security system;

(d)   retrieving, via said security system, said security information of said verified user from said storage unit; and

(e)   receiving said identified security information from said security module at said security system and negotiating communication parameters for said network interface with said secure web server utilizing said retrieved security information to facilitate said secure encrypted session between said secure web server and said voice browser.

21.   The method of claim 20 wherein said network includes the Internet.

22.   The method of claim 20 wherein said network interface is in communication with a communications device located remotely of said network interface, and step (a) further includes:

(a.1)   retrieving said user voice signals from said communications device.

23.   The method of claim 22 wherein said communications device includes a telephone.

24.   The method of claim 22 wherein said communications device includes a computer system having an audio input device.

25.   The method of claim 24 wherein said audio input device includes a microphone.

26.   The method of claim 20 wherein step (a) further includes:

(a.1) providing said user information to said security system to facilitate verification of said user in response to a request from said security system for user information;

(a.2) receiving verification results from said security system and providing said verification results to said user;

(a.3) providing said identified security information to said security system to facilitate negotiation of said communication parameters;

(a.4) receiving responses to said identified security information and said negotiated communication parameters from said security system; and

(a.5) providing said responses and said negotiated parameters to said network interface to facilitate secure communications over said network between said secure web server and said voice browser.

27. The method of claim 26 wherein step (c) further includes:

(c.1) validating an identification within said user information associated with an authorized user;

(c.2) retrieving said voice information from said storage unit associated with said identification;

(c.3) selecting portions of said retrieved voice information and generating said user information request, wherein said generated request includes a request for user information corresponding to said selected portions of said retrieved voice information; and

(c.4)   verifying said user by comparing said user voice signals received from said security module in response to said user information request with said stored voice information associated with an authorized user identified by said identification and providing said verification results to said security module; and

step (e) further includes:

(e.1)   processing said identified security information received from said security module and generating said responses thereto with said retrieved security information to negotiate said communication parameters; and

(e.2)   providing said responses and negotiated parameters to said security module to facilitate secure communications over said network between said secure web server and said voice browser.

28.   The method of claim 20 wherein said storage unit includes a database.

29.   The method of claim 21 wherein said stored security information includes private keys and certificates of said authorized users.

30.   The method of claim 20 further including the step of:

(f)   retrieving voice signals from said authorized users and processing said authorized user voice signals to produce said voice information for storage in said storage unit.

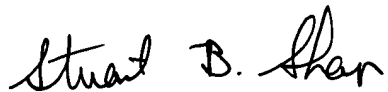(9) <u>Evidence Appendix</u>

None.

(10)   <u>Related Proceedings Appendix</u>

None.

(11)   Conclusion

In view of the foregoing, it is submitted that the final rejections of claims 1 - 30 are improper

and, accordingly, the Board is respectfully requested to reverse the final rejections and order that this

application be allowed.

Respectfully submitted,

Stuart B. Shapiro
Registration No. 40,169

EDELL, SHAPIRO & FINNAN, LLC
1901 Research Boulevard, Suite 400
Rockville, Maryland 20850
(301) 424-3640

Hand-delivered: 8-2-2006